possible to confirm later the correct processing of questioned transactions, as for example when the recipient denies receiving a message. With adequate audit trails, the sender can show the sequence of messages sent to the recipient, including the repudiated message, with acknowledgment of delivery by the network, and receipt by the recipient. Likewise, recipient applications should maintain audit trails to be able to demonstrate timely processing and acknowledgment of transactions.

If the EDI system fails, a transactions audit trail can be used to determine which transactions were lost by the EDI system; these transactions would need to be re-entered.

3.4 Techniques for the EDI System

This section presents good security practices that apply generally to the EDI part of an EC system.

3.4.1 Use of Standard Transaction Sets

As noted in Section 1.5.1 of this report, FIPS PUB 161-1, Electronic Data Interchange, "adopts, with specific conditions, the families of standards known as X12 and EDIFACT." and requires the use of these transaction sets if they meet "the data requirements" of Federal agencies implementing EC systems. Since these standards have been carefully developed to ensure reliable, accurate EC, this requirement is a good security practice that all designers of EC systems should follow. Similarly, system designers should follow Section 8.4 of FIPS PUB 161-1 when designing a new transaction set when no X12-defined transaction set is yet available to perform a required function.

Section 10.4 of FIPS PUB 161-1 also specifies that X12 versions and releases should not be used after a period of time, provided that they are replaced by newer versions and releases. The intent of this requirement is to keep all trading partners current with similar versions, to minimize differences in software when a system of trading involves many partners.

3.4.2 Rejection of Invalid Transactions Without Correction

The EDI translation program should not attempt to correct invalid input from the sender's application.

The structure of the input from the sender's applications is communicated to the EDI translation program through tables, sometimes called maps, that relate data fields in the applications to the data elements of the corresponding EDI transaction sets. All applications must supply the required kind of data, for example, a number, a date, a text string, etc., or a default value for all the data elements. If an error occurs either because there is an error

in the map, or the application generates an invalid data field, the cause of the error should be identified and corrected. Attempts by the translation program to correct such errors will obscure the error condition, and the correction may not be made correctly. In particular, EDI system personnel should not under any circumstances edit input data. Otherwise separation of duties is lost, and corrections may be faulty. For all these reasons, invalid input should be rejected without exception.

The translation of transactions must be accurate and complete. A key step in the design of an EC system is to compare systematically the data fields in the sender's application output with the data elements defined for the target transaction set. If any data elements are missing, the sender's application must be modified to add the missing information, or suitable default values established. Finally, the action of the translation program should be tested exhaustively to validate the implementation of the program.

3.4.3 Maintenance of Audit Trails

The audit trails required to permit reconciliation by the application with the EDI system should be maintained, to support recovery from contingencies, and to support non-repudiation.

Facilities and procedures should be provided to report back to the applications the status of transactions processed. This enables the applications to detect lost, mishandled, or duplicated messages, and to recover from EDI system breakdowns.

Facilities, procedures, and controls, including back-up of input and output files and transaction logs, should be provided as required to ensure timely and accurate recovery from EDI system and network failures without omitting or duplicating messages.

The EDI system should maintain transaction logs that make it possible to confirm correct processing of questioned messages, as for example, if and when the recipient denies receiving a message.

3.4.4 Reliable Network Interface

The network interface must provide facilities to protect against duplication of messages by inadvertent retransmission of a message to the network. The EDI system must ensure that each message generated by the translator program is delivered only once to the network interface, and that every message received from the network is processed by the translation program only once.

The EDI system should monitor the response time of the network, and generate an alarm promptly if response falls below the expected level.

3.5 Techniques for the Network

The EC system design should include the required performance specifications for the network, including the level of required security. Whether the network is operated by one or more of the trading partners, or by a third party, the network should be treated as a separate entity. Thus, the same security and control considerations apply regardless of the reporting structure.

3.5.1 Network Acceptance Criteria

The trading partners should verify that a proposed network satisfies the EC system's technical specifications. In addition, the partners should be assured that the operation of the network will be in compliance with desired security and control procedures, and that the size and competence level of the network staff is adequate to deal with technical faults and emergencies, and requests for assistance from users.

3.5.2 The Network Usage Agreement

Acceptance of a network must include the execution of a network usage agreement with network management. A common network usage agreement should be used by all the trading partners to ensure that all partners have the same understanding of how the network will function as a part of the EC system.

If trading partners are using different networks that interconnect, it will be important for the usage agreements to consider the issues of joint data transmission, and joint contingency plans and recovery. Both networks must work together for the EC system to be operative.

3.5.3 Access Controls

A network should provide an effective system of access control and management. This system should include a system for assignment, change, and revocation of identifications and passwords used to access the network and its mailboxes. See also Section 3.6.

3.5.4 Treatment of User Messages

1) Editing of messages

Under no circumstances should network personnel be permitted to alter messages. This situation may arise specifically if a trading partner contracts with a VAN to perform the translation function.

Networks should apply checks to detect corruption of messages that occur before delivery to the recipient. However, it is not a good security practice to have network personnel edit messages that are rejected by translation software. If message corruption does

occur, the corrupted message should never be edited. Instead, the message should be restored from a back-up copy, or the sender should be asked to retransmit it. While this activity may delay messages, permitting network personnel to perform such edits is a major control weakness.

2) Retention of Messages

Retention of EDI messages by a network should be brief.

Networks should not retain back-up copies of messages any longer than is reasonably necessary to permit recovery from service interruptions. In most circumstances it should not be necessary to retain any copy of a message for more than a week. This practice minimizes the extent to which messages are outside the control of the trading partners.

3) Access To EDI Messages

Access to EDI messages by network personnel should be controlled.

Network personnel should not be able to access the text of EDI messages except as absolutely necessary to ensure proper technical operation of the network. The network should have controls that ensure that all such accesses are only made by authorized personnel, and are recorded.

4) Log of Messages

A network should maintain a transaction log of messages sufficient to permit later verification of the delivery of a specific message from a sender to a recipient to support non-repudiation. The retention period of these logs should satisfy legal requirements.

5) Controlled Delivery of Messages

A network should maintain for each user a table of other network users who are authorized recipients of messages. The network should reject messages addressed to non-specified recipients.

3.5.5 Protection of Network Terminations

Adequate physical security to network communications circuits should be provided at trading partner premises.

Every network is especially exposed to wire tapping and sabotage at the point where network communications circuits leave trading partner premises, since it is relatively easy to identify the specific circuits carrying the network traffic. Consequently, if there is a significant risk of wire tapping or sabotage, adequate physical access controls should be imposed on the network terminations located on trading partner premises.

3.5.6 Contingency Plan

A network should have a contingency plan that is consistent with the service reliability objectives. The contingency plan should be tested regularly. Since the conduct of EC is totally dependent on the operation of the network(s), it is essential to determine how operation will be resumed promptly if there is a network outage that is expected to last longer than the maximum acceptable service interruption. The risk analysis of an EC system should yield an estimate of the dysfunctional cost of a network outage as a function of the duration of the outage. An estimate should be prepared of the annual standby cost to maintain the capability to restore service using alternate facilities as a function of the time required to restore service. The optimum recovery time is probably the one with the lowest total of risk and standby costs.

Since the conduct of EC is totally dependent on the operation of the network, it is essential to demonstrate regularly the ability of the network to recover within the stipulated time. Regular tests of network contingency plans should be conducted. The usage agreement should specify how this testing is to be done. The trading partners should verify that the conduct and results of tests comply with the terms of the agreement.

3.5.7 Network Audits

A network should be subject to regular internal control audits by a technically qualified independent activity (not directly involved in the operation of the network) to ensure that appropriate controls and checks are in place, and that there is compliance with them. The usage agreement should specify how audits are to be conducted. The agreement should provide for the trading partners to receive copies of the audit reports directly from the audit activity, as well as copies of documents describing resolution of deficiencies enumerated in audit reports.

3.6 User Authentication and Access Controls

Logical access to the functions of an EC system should be controlled by a properly administered system of user authentication employing adequate facilities and personnel.

There are five EC system functions that should require user authentication as follows:

1) Access to the network to initiate transmit or receive EDI messages;

2) Access to the EDI system to control its operation or to update operating parameters;

3) Access to an application to control operation and initiate transactions;

4) Affixing an individual signature to a transaction; and

5) Initiation of an encrypted transmission.

As a minimum, the EC system design should provide for use of user IDs and passwords for each of the functions. If the risk analysis reveals an unusually high level of risk, consideration should be given to more secure techniques to authenticate individual users.

The security benefit of a password system depends entirely on the thoroughness with which passwords are administered. There have been numerous examples of how easily intruders have been able to break into systems where administration of passwords was weak. Appendix E of FIPS PUB 112, Password Usage, provides a detailed and authoritative discussion of password management. This appendix is based on the password management guidelines developed by the DoD Computer Security Center, and presents good practices for the administration of authentication based on user IDs and passwords. See also the more recent FIPS PUB 181, Automated Password Generator. Features presented in these documents should be applied to the daily operation of the EC system's authentication mechanism.

3.7 Electronic Document Management

A system of electronic document management should be provided such that all required business documents that are in electronic form are retained, stored, and indexed to satisfy operational, audit, and legal requirements.

The substitution of electronic documents for paper documents does not change the business and legal requirements for documents, whatever their medium. The development of the concept of electronic document management is a formal recognition of the requirement to be able to use electronic documents just as easily and confidently as paper documents. Several electronic document management concepts must be addressed during the design of an EC system:

1) Assurance of retention of all relevant documents.

2) An index system to allow prompt retrieval.

3) The dependability and effective life of storage media.

4) Protection of stored documents against unauthorized access, modifications, and disclosure.

5) Implementation of an audit trail including dates and times for recording additions, deletions, and alterations.

6) Document retention times and timely destruction of superfluous copies of documents.

3.8 Maintenance of Audit Trails

The discussion of electronic documents above makes it clear that record systems must be implemented to enable documents to be easily retrieved. Likewise it is important to be able to reconstruct the sequence of events when an error condition arises. Finally, EC can be expected to weaken the effectiveness of separation of duties as an anti-fraud control. For all these reasons, it is important to be sure that the applications and the EDI system create and maintain adequate audit trails and transaction journals. The system analysis and the risk analysis should both stress the need to identify the audit trail requirements.

In those cases where an audit trail is particularly valuable, consideration should be given to the use of techniques that chain records in sequence to prevent insertion or deletion of individual records. Such a requirement could arise in a defense against repudiation.

Since there may be substantial automatic resolution of error conditions, it is prudent to maintain a separate log of all such resolutions. If the error rate increases significantly, an exception condition requiring human intervention should be generated. Otherwise, recognition of a source of errors may be unduly delayed.

3.9 Contingency Planning

An adequate contingency plan for the EC system should be provided.

3.9.1 Development of a Cost-Effective Plan

The risk analysis of a planned EC system should yield an estimate of the expected losses (ALEs) associated with outages of each of the applications, the EDI system, and the entire EC system. If the TPA holds one trading partner responsible for the effects on other partners of an in-house service interruption, it will be necessary to include the effect of outages on other trading partners as well as the in-house effects. The ALE estimates should be stated as a function of the duration of the service interruptions. This information can then be used to identify the most cost-effective contingency plan for each application, the EDI system, and the entire EC system.

3.9.2 Plan Objective

The objective of the contingency plan is to ensure timely and accurate recovery from service interruptions, and events that

destroy hardware and data files. Timely recovery means that the maximum (worst case) outage will not cause excessive service interruption losses to any trading partner, and that performance standards in the TPA regarding timeliness will be met. Accurate recovery means that no transactions are lost or duplicated. By designing the contingency plan at the same time as the EC system itself, consideration can be given to the question of timely replacement of destroyed hardware, and the frequency with which files are backed up for on-site and off-site storage.

3.9.3 Functioning of the Plan

Adequate EDI system resources and personnel should be provided under the contingency plan to ensure prompt response to trouble and exception reports, and to requests for assistance from trading partners.

The size and competence level of the EDI system staff must be adequate to deal with emergencies and technical faults on time. Since EDI system failures have the potential to interrupt all EC transactions into and out of the organization, it is important to be sure that the EDI staff has the resources and training to deal effectively with emergencies. These considerations apply to a lesser extent to the operators of the applications.

In some cases, an EC system will involve a large, dominant trading partner and many small trading partners who participate at the request of the dominant partner. In such a situation, there are two important considerations.

The first is that an EDI system failure at the dominant partner may prevent timely performance by all the small trading partners. This is particularly important if the dominant partner is a Federal Government agency and the small trading partners make required filings through the EC system. The dominant partner should establish a policy at the time the EC system is introduced that defines how service interruptions at the dominant partner facility will affect the requirement for timely filings prescribed for the small partners. The policy should be included in the TPA.

The second consideration is that small trading partners may lack the breadth of in-house resources needed to deal effectively with exception conditions and emergencies that affect their EC systems. Since it is in the interest of the dominant partner to ensure smooth operation, the dominant partner should consider the value of providing a "help desk" service for the small trading partners.

As a minimum, the TPA should require all partners to maintain a roster of names (or functional titles) and telephone numbers of staff members trained and designated to deal with potential problems, and provide the other partners with a copy. These lists could be distributed as EDI messages that could be used to update

an automated "help desk" function that is a part of the EC system. Thus, a small trading partner who encounters a problem, can determine exactly who to contact for help.

3.9.4 Contingency Plan Tests

Regular testing of the contingency plans should be carried out to ensure that EC system performance commitments can be met. Experience with conventional data processing systems has shown that regular testing is essential to the effectiveness of a contingency plan. Tests perform three functions:

1) Staff members receive on-the-job training in the operation of the contingency plan.

2) Deficiencies in the plan are discovered, and corrective action is taken before an emergency arises.

3) Each trading partner can be assured of the ability of the other partner(s) to meet agreed to timeliness goals. Indeed, a requirement for regular testing should be a part of the TPA for just this reason.

3.10 EC System Compliance Audits

EC systems should be subject to regular internal control audits by a technically qualified independent activity (not directly involved in the operation of the EC system) to ensure that appropriate controls and checks are in place, and that there is compliance with them.

For all these reasons, the effectiveness of the security measures, controls, logs, and audit trails are even more important than they are for a traditional business system. Consequently, effective auditing to identify control weaknesses and failures to comply with controls is of increased importance.

Careful design and testing are intended to ensure that controls are adequate, but controls cannot reasonably be expected to work flawlessly when first put into operational use. Likewise, changing circumstances may weaken controls or lead to the requirement for new controls. Effective auditing will disclose such weaknesses and deficiencies.

The EC system implementation plan should ensure that the training of staff members during initial implementation is adequate to ensure both proper routine operation and, more importantly, correct responses to exception conditions. However, the initial training may not be completely effective, and personnel may be reassigned after initial training is completed. Finally, experience shows that, unfortunately, some staff members will violate the trust

placed in them under some circumstances. The nature of EC suggests that in some cases, fraud losses could be significantly higher than with traditional business systems.

For all these reasons, it is important to audit regularly for compliance with controls by staff members. Expediency is a poor reason for violating controls, and it may create a climate where dishonesty becomes more difficult to detect.

Verification of the integrity of the transaction logs and electronic document files is a key part of the audit program. These records are essential to the management of EC, the settlement of exceptions, and the resolution of repudiation by a trading partner.

The results of the EC system risk analysis should provide the basis for determining the appropriate level and detail of the audit program. This is done by balancing the expected level of losses as a function of the level (scope and detail) of the audit program against the cost to conduct the audit at each level. This analysis will provide an economic basis for the conduct of the audits by stressing the impact on security and efficiency.

3.11 Testing

The processing of all incoming and outgoing transaction sets should be thoroughly tested before live operation is begun.

Great care must be taken in the design and conduct of tests. Testing should proceed step by step. Tests should first verify that each application generates the expected output information for the EDI system. Next, the EDI translation software should be tested to verify that valid EDI transaction sets are generated for each of the application inputs. Following this, tests should be undertaken to verify that the EDI system constructs correct interchange envelopes. Finally, after both trading partners have completed the preceding tests, tests should be conducted together to verify correct end-to-end handling of EDI messages. Each transaction should be tested for: (a) boundary conditions of all input data fields, (b) error conditions such as invalid part numbers, dates, quantities, and prices, and null transactions, (c) failures to acknowledge, and (d) negative acknowledgments.

The system designers should not design or conduct the tests. Independent testers should design the tests based on the system specifications, with the goal of demonstrating that the systems work as intended, regardless of errors and omissions.

It is also critical to verify correct handling of potential overload conditions at month-end, quarter-end, and year-end when traffic levels may be abnormally high, and timeliness may be especially important.

Since EC between partners is likely to expand and evolve as the benefits of EC are realized, it is important to include permanent testing facilities in the design of systems. An EDI system should be able to distinguish test messages from operational messages.

Case Study: A EDI systems programmer, intending to perform a test, logged onto a network mailbox. He was surprised when the network automatically uploaded 1,200 pending messages into a test file instead of into the appropriate EDI system input storage area. The system programmer was not able to recover the messages, and it was necessary to have the messages retransmitted.

To avoid problems like this, VAN users may want to maintain a test mailbox to which system programmers can send test messages for subsequent retrieval. This is analogous to a local loop-back test on a communications circuit.

APPENDIX A: ABBREVIATIONS AND ACRONYMS

ALE	Annualized Loss Expectancy
ANSI	American National Standards Institute
ASC X12	Accredited Standards Committee X12
DISA	Data Interchange Standards Association
DoD	U.S. Department of Defense
DSA	Digital Signature Algorithm
EC	Electronic Commerce
EDI	Electronic Data Interchange
EDIFACT	EDI For Administration, Commerce and Transport
EFT	Electronic Funds Transfer
FIPS PUB	Federal Information Processing Standards Publication
IDs	Personal Identifications
NBS	National Bureau of Standards (now NIST)
NIST	National Institute of Standards and Technology
QRA	Quantitative Risk Analysis
RFQ	Request For Quotation
SHA	Secure Hash Algorithm
SOL	Single Occurrence Loss
TPA	Trading Partner Agreement
VAN	Value-Added Network
X12	See ASC X12

APPENDIX B: BIBLIOGRAPHY

American Bar Association, Section on Business Law, Electronic Messaging Services Task Force, "Model Electronic Data Interchange Trading Partner Agreement and Commentary," Business Lawyer, Vol. 45, p. 1717. 1990.

Baum, Michael and Henry Perritt, Jr. Electronic Contracting, Publishing and EDI Law. John Wiley & Sons, New York, NY. 1991.

Data Interchange Standards Association. 1993 DISA Publications Catalog. Alexandria, VA. 1993.

Gilbert, Irene E. Guide for Selecting Automated Risk Analysis Tools. NIST SP 500-174. National Institute of Standards and Technology. Gaithersburg, MD. 1989.

Helsing, Cheryl, Marianne Swanson and Mary Anne Todd, Computer User's Guide to the Protection of Information Resources. NIST SP 500-171. National Institute of Standards and Technology. Gaithersburg, MD. 1989.

National Bureau of Standards. FIPS PUB 65, Guideline for Automated Data Processing Risk Analysis. Gaithersburg, MD. 1979.

National Bureau of Standards. FIPS PUB 87, Guidelines for ADP Contingency Planning. Gaithersburg, MD. 1981.

National Bureau of Standards. FIPS PUB 112, Standard on Password Usage. Gaithersburg, MD. 1985.

National Bureau of Standards. FIPS PUB 113, Standard on Computer Data Authentication. Gaithersburg, MD. 1985.

National Institute of Standards and Technology. CSL Bulletin: Security Issues in the Use of Electronic Data Interchange. Gaithersburg, MD. June, 1991.

National Institute of Standards and Technology. CSL Bulletin: Digital Signature Standard. Gaithersburg, MD. January, 1993.

National Institute of Standards and Technology. FIPS PUB 46-2, Data Encryption Standard (DES). Gaithersburg, MD. 1993.

National Institute of Standards and Technology. FIPS PUB 161-1, Electronic Data Interchange. Gaithersburg, MD. 1993.

National Institute of Standards and Technology. FIPS PUB 180, Secure Hash Standard. Gaithersburg, MD. 1993.

National Institute of Standards and Technology. FIPS PUB 181, Automated Password Generator. Gaithersburg, MD. 1993.

Roback, Edward, NIST Coordinator. U.S. Department of Justice Simplified Risk Analysis Guidelines (SRAG). Gaithersburg, MD. 1990.

Saltman, Roy G., editor. Workshop on Security Procedures for the Interchange of Electronic Documents: Selected Papers and Results. NISTIR 5247. National Institute of Standards and Technology. Gaithersburg, MD. 1993.

Troy, Eugene F. Security for Dial-Up Lines. NBS SP 500-137. National Bureau of Standards. Gaithersburg, MD. 1986.

Wright, Benjamin. EDI and American Law: A Practical Guide. The Electronic Data Interchange Association. Alexandria, VA. 1989.